FRAUD ALERTS • FRAUD ALERTS • FRAUD ALERTS

Protect Yourself From Scams

The following are some of the most common scams perpetrated against seniors. Read on to familiarize yourself with these schemes and protect your finances.

IRS Scam Calls

A scam artist claims to be from the IRS and tells the caller they owe back taxes. Money must be paid immediately through a prepaid debit card or wire transfer to avoid arrest or legal consequences. The scammers spoof numbers to appear to be calling from the Washington, DC, area code 202.

Grandparents Scam

Scam artists claiming to be attorneys, paralegals and law enforcement officers frantically call saying that a grandchild is in trouble and requesting the grandparent immediately wire money or send a prepaid debit card.

Prizes/Sweepstakes/Free Gifts Scam

A scam artist mails a letter or calls you and pretends to be with Reader's Digest, Publisher's Clearing House, a government agency or a phony foreign lottery. The scam artist claims that you have "won" money and tells you that you must wire hundreds or even thousands of dollars to the scam artist to cover taxes or some other bogus fees. You wire money or send a prepaid debit card, but the prize never arrives.

Home Improvement/Doorstep Scam

A scam artist knocks on your door offering to repair something in or around your home. They ask you to pay upfront and you never see the alleged repairman again.

Charity Scam

A caller claims to collect money for needy children, veterans, or victims of a recent disaster. Always research charities before making a donation to ensure that the charity is registered with the Attorney General's office as required by law.

Mortgage/Reverse Mortgage Scam

A con artist offers you a free home, investment opportunities, or mortgage foreclosure or refinancing assistance. You may hear about such schemes through investment seminars as well as via television, radio, billboard, and mailer advertisements, and even from people you know.

Computer Tech Support Scam

The scammers may call or send an email offering to help solve your computer problems or sell you a software license. Once they are given access to your computer, they can install malicious software that can capture sensitive data, such as online banking user names and passwords; try to control your computer remotely and adjust settings to leave your computer vulnerable; request credit card information so they can bill you for phony services; or direct you to fraudulent websites and ask you to enter credit card or other personal or financial information there.

Phishing/Spoofing Scam

Scam artists claiming to represent government agencies, local utilities, charities, banks or law enforcement call, mail, email or make door-to-door solicitations requesting your personal information.

Wandering Contractors Scam

A scam artist comes to your door and pretends that you have a tree that needs trimming or a roof in need of repair to distract you while another person sneaks into your home to steal cash and valuables.

Investment/Ponzi Scheme

A scam artist encourages you to make investments and promises unrealistically high returns.

Friendship/Sweetheart Scam

A scam artist nurtures an online relationship, building trust and confidence, then convinces you to send money.

Work-At-Home Scam

A scam artist promises you big money to work from home assembling products, establishing an online business, or mystery shopping. You may invest hundreds of dollars for start-up with little, if any, return in payment.

Free Trial Offer Scam

A scam artist uses television advertisements and unwanted telephone calls offering free goods and services and then asks for your credit card information. Time passes and you don't realize that you are being billed every month for that free trial offer.

Bereavement Scam

Scammers often try to take advantage of senior citizens who have recently lost a loved one, such as a spouse. Scammers call, claim that the deceased spouse has outstanding debts that must be paid immediately, and ask for a blank check or credit card information for payment.

Illinois Attorney General Consumer Fraud Hotlines

Chicago	Springfield	Carbondale
800-386-5438	800-243-0618	800-243-0607
800-964-3013 (TTY)	877-844-5461 (TTY)	877-675-9339 (TTY)

A Message From Illinois Attorney General Lisa Madigan

According to the U.S. Department of Education, 81% of children as young as 3 years old are now using the Internet.

With the majority of today's kids online, parents and guardians are understandably concerned about Internet safety, but they may not know what steps they should take to protect their children.

Fortunately, the answer is not as difficult as you might think. You cannot watch your kids every minute, but you can use strategies to help them benefit from the Internet and avoid its potential risks. Perhaps the most important thing you can do to promote online safety is to talk with your kids about the rewards and potential risks of Internet use.

By providing guidance for your children, you can expand their online skills and confidence, and you can help them learn to avoid potential risks. And you might be surprised by what they teach you at the same time!

Lisa Madigan

Lisa Madigan
Attorney General

Additional online safety resources are available from NetSmartz411® at www.NetSmartz411.org or 1-888-NETS411 (638-7411).

For more information, please contact our office:

CHICAGO
100 W. Randolph Street
Chicago, IL 60601
312-814-3000
TTY: 1-800-964-3013

SPRINGFIELD
500 S. Second Street
Springfield, IL 62706
217-782-1090
TTY: 1-877-844-5461

CARBONDALE
601 S. University Avenue
Carbondale, IL 62901
618-529-6400
TTY: 1-877-675-9339

www.ebully411.com
www.IllinoisAttorneyGeneral.gov

ILLINOIS ICAC
OFFICE OF THE ILLINOIS ATTORNEY GENERAL

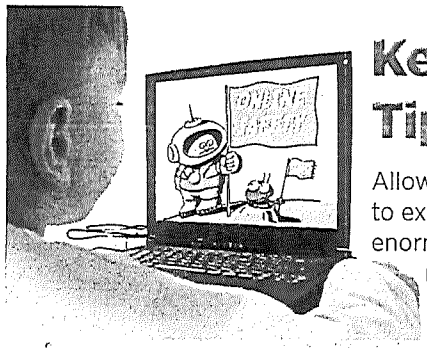
Printed by Authority of the State of Illinois.
This material is available in alternate format upon request.
Reprinted with permission from National Center for Missing and Exploited Children.

Keeping Kids Safer Online

Minimizing Risks While Developing Online Skills

Internet Crimes Against Children Task Force

LISA MADIGAN
Illinois Attorney General



Keeping Kids Safer on the Internet: Tips for Parents and Guardians

Allowing kids to go online without supervision or ground rules is like allowing them to explore a major metropolitan area by themselves. The Internet, like a city, offers an enormous array of entertainment and educational resources, but also presents some risks. Kids need help navigating this world. Here's how parents and guardians can help:

Where Do Kids Connect?

In general, kids:

- Connect to the Internet from a computer at home, at school, or at a library or a friend's home.
- Connect from anywhere using laptops, cell phones, handheld devices and other wireless devices.
- Compete against and chat with players around the world using Internet-enabled gaming systems.
- Exchange messages, photos and videos via the Internet at any time.

Ways to Enhance Kids' Online Skills

- Begin a dialogue with your kids about Internet use.
- Consider rating, blocking, monitoring and filtering applications.
- Make Internet use a family activity while encouraging critical thinking.
- Set reasonable rules including time limits.
- Encourage your kids to go to you when they encounter problems online.

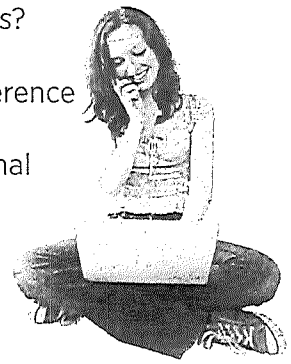
More Tips to Minimize Risks

- Instruct your kids to use privacy settings to restrict access to profiles so only the individuals on their contact lists are able to view their profiles.
- Remind kids only to add people they know in real life to their contact lists.
- Encourage kids to choose appropriate screen names or nicknames.
- Talk to your kids about creating strong passwords, such as those that use the first letter of each word of a phrase or an easy-to-remember acronym.
- Visit social networking sites with your kids, and exchange ideas about which sites pose potential risks.
- Ask your kids about the people they communicate with online. Help them learn how to make choices about who is appropriate to friend.
- Make it a rule with your kids that they can never give out personal information or meet anyone in person without your prior knowledge and consent. Define "personal information" with your child.
- Encourage your kids to think, "Is this message harmful, dangerous, hurtful or rude?" before posting or sending anything online.
- Teach your kids not to respond to any rude or harassing remarks or messages that make them feel scared, uncomfortable or confused and to show you these messages instead.

Kids' Corner

You can't take it back ... Think before you type!

- ✓ Is my online content hurtful, rude, dangerous or harmful?
- ✓ Would I want a parent, guardian, grandparent or trusted adult to see my post?
- ✓ Would I want someone to treat me this way?
- ✓ What are the consequences of what I post?
- ✓ How will online content affect my future education, employment, military involvement or relationships?
- ✓ How do I know this person? Family, friend, acquaintance or stranger?
- ✓ How do the qualities of my real-life friends compare to my online friends?
- ✓ What is the difference between writing secrets in a journal versus online?



ILLINOIS ATTORNEY GENERAL

Consumer Fraud Hotlines

1-800-386-5438 (Chicago)
1-800-243-0618 (Springfield)
1-800-243-0607 (Carbondale)

Toll-Free TTY Numbers

1-800-964-3013 (Chicago)
1-877-844-5461 (Springfield)
1-877-675-9339 (Carbondale)

Identity Theft Hotline

1-866-999-5630
1-877-844-5461 (TTY)

Senior Citizen Consumer Fraud Hotline

1-800-243-5377

MAIN OFFICES		
Chicago Main Office 100 West Randolph Street Chicago, IL 60601 (312) 814-3000 TTY: 1-800-964-3013	**Springfield Main Office** 500 South Second Street Springfield, IL 62706 (217) 782-1090 TTY: 1-877-844-5461	**Carbondale Main Office** 601 South University Ave. Carbondale, IL 62901 (618) 529-6400/6401 TTY: 1-877-675-9339
REGIONAL OFFICES		
Chicago West Regional Office 306 N. Pulaski Rd. Chicago, IL 60624 (773) 265-8808 TTY: 1-866-717-8804	**East Central Illinois Regional Office** 1776 E. Washington St. Urbana, IL 61802 (217) 278-3366 TTY: (217) 278-3371	**Chicago South Regional Office** 8100 S. Stony Island, Suite C Chicago, IL 60617 (773) 768-5926 TTY: (866) 717-8798
REGIONAL OFFICES (continued)		
Northern Illinois Regional Office Zeke Giorgi Center 200 South Wyman St. Suite 307 Rockford, IL 61101 (815) 967-3883 TTY: (815) 967-3891	**West Central Illinois Regional Office** 628 Maine Street Quincy, IL 62301 (217) 223-2221 TTY: (217) 223-2254	**Metro East Illinois Regional Office** 201 West Pointe Drive Suite 7 Belleville, IL 62226 (618) 236-8616 TTY: (618) 236-8619

EQUIFAX experian TransUnion

Annual Credit Report Request Form

You have the right to get a free copy of your credit file disclosure, commonly called a credit report, once every 12 months, from each of the nationwide consumer credit reporting companies - Equifax, Experian and TransUnion.

For instant access to your free credit report, visit www.annualcreditreport.com.

For more information on obtaining your free credit report, visit www.annualcreditreport.com or call 877-322-8228.

Use this form if you prefer to write to request your credit report from any, or all, of the nationwide consumer credit reporting companies. The following information is required to process your request. **Omission of any information may delay your request.**

Once complete, fold (do not staple or tape), place into a #10 envelope, affix required postage and mail to:

Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281.

Please use a Black or Blue Pen and write your responses in PRINTED CAPITAL LETTERS without touching the sides of the boxes like the examples listed below:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

Social Security Number: ___ - ___ - ____

Date of Birth: ___ / ___ / ____ (Month / Day / Year)

Fold Here — Fold Here

First Name ____ M.I. ____

Last Name ____ JR, SR, III, etc. ____

Current Mailing Address:

House Number ____ Street Name ____

Apartment Number / Private Mailbox ____ For Puerto Rico Only: Print Urbanization Name ____

City ____ State ____ ZipCode ____

Previous Mailing Address (complete only if at current mailing address for less than two years):

House Number ____ Street Name ____

Fold Here — Fold Here

Apartment Number / Private Mailbox ____ For Puerto Rico Only: Print Urbanization Name ____

City ____ State ____ ZipCode ____

Shade Circle Like This → ●

Not Like This → ⊗ ✓

I want a credit report from (shade each that you would like to receive):

- ○ Equifax
- ○ Experian
- ○ TransUnion

○ **Shade here if, for security reasons, you want your credit report to include no more than the last four digits of your Social Security Number.**

If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

31238

G-1

Federal Trade Commission – OPT OUT

Please select from the options listed below to Opt-Out of lists supplied by Equifax, Experian, Innovis and TransUnion for firm offers of credit or insurance. If you have previously completed a request to Opt-Out from receiving firm offers and would like to Opt-In, you may also complete your request on this website.

To exercise your right to Opt-Out of firm offers of credit and insurance, you'll be asked to provide your personal information set out below.

- Name
- Address
- Social Security Number
- Date of Birth

Your Social Security Number and Date of Birth are not required to process your request. However, providing this information will help to ensure that we can successfully process your request. This website's security protocols and features are designed to protect your personal information from unauthorized access or alteration. As an added security measure, we only display the last four digits of your Social Security Number on the confirmation screen. If you do not provide your Social Security Number, we will attempt to process your request without this information. Once you click submit, you will be prompted to enter your personal information. You will have 15 minutes to complete your request.

○ **Opt-In:**	Your name will be eligible for inclusion on lists used for Firm Offers of credit or insurance.
○ **Electronic Opt-Out for Five Years:**	Your name will not be eligible for inclusion on lists used for Firm Offers of credit or insurance for five years.
○ **Permanent Opt-Out by Mail:**	Your name will no longer be eligible for inclusion on lists for Firm Offers of credit or insurance (In order to complete your Permanent Opt-Out election, you must print and mail the Permanent Opt-Out Election form.

What is Permanent Opt-Out by Mail?

Opting-Out refers to the process for removing your name from lists supplied by the Consumer Credit Reporting Companies, Equifax, Experian, Innovis and TransUnion, to be used for firm (preapproved / prescreened) offers of credit or insurance. Your rights as a consumer under the Fair Credit Reporting Act (FCRA) include the right to "Opt-Out" for **5 years or permanently.**

If you choose permanent Opt-Out, you must "confirm" your request in writing by submitting a signed Permanent Opt-Out Election form. At the time that you submit your electronic request, you will receive a confirmation that you should print along with the Permanent Opt-Out Election Form. You may begin the permanent Opt-Out process on this secure website, however, in order to complete your request, you must return the signed Permanent Opt-Out Election form. The Permanent Opt-Out Election form will be provided to you after you initiate your request on this website. In the interim, we will complete a 5 year Opt-Out request on your behalf within 5 business days. We will make your request permanent when we receive your signed Permanent Opt-Out Election form.

If you don't have access to the Internet, you may send a written request to permanently opt out to each of the major consumer reporting companies. Make sure your request includes your home telephone number, name, Social Security number, and date of birth.

Experian
Opt Out
P.O. Box 919
Allen, TX 75013

TransUnion
Name Removal Option
P.O. Box 505
Woodlyn, PA 19094

Equifax, Inc.
Options
P.O. Box 740123
Atlanta, GA 30374

Innovis Consumer Assistance
P.O. Box 495
Pittsburgh, PA 15230

Direct Marketers

Telemarketing

The federal government's National Do Not Call Registry is a free, easy way to reduce the telemarketing calls you get at home. To register your phone number or to get information about the registry, visit www.donotcall.gov, or call 1-888-382-1222 from the phone number you want to register. You will get fewer telemarketing calls within 31 days of registering your number. Telephone numbers on the registry will only be removed when they are disconnected and reassigned, or when you choose to remove a number from the registry.

Mail

The Direct Marketing Association's (DMA) Mail Preference Service (MPS) lets you opt out of receiving unsolicited commercial mail from many national companies for five years. When you register with this service, your name will be

put on a "delete" file and made available to direct-mail marketers and organizations. This will reduce most of your unsolicited mail. However, your registration will not stop mailings from organizations that do not use the DMA's Mail Preference Service. To register with DMA's Mail Preference Service, go to www.dmachoice.org, or mail your request with a $1 processing fee to:

DMAchoice
Direct Marketing Association
P.O. Box 643
Carmel, NY 10512

Email

The DMA also has an Email Preference Service (eMPS) to help you reduce unsolicited commercial emails. To opt out of receiving unsolicited commercial email from DMA members, visit www.dmachoice.org. Registration is free and good for six years.

Placing a freeze on your credit report will prevent lenders and others from accessing your TransUnion Credit Report entirely, which will prevent them from extending credit. With a Security Freeze in place, even you will need to take special steps when you wish to apply for any type of credit. Because of more stringent security features, you will need to place a Security Freeze separately with each of the three major credit reporting companies if you want the freeze on all of your credit files. A Security Freeze remains on your credit file until you remove it or choose to lift it temporarily when applying for credit or credit-dependent services.

Need/interest: - You want maximum control of your credit - You are concerned that you might become a victim of fraud/ID theft - You are a victim of fraud/ID theft - You won't need to apply for credit in the foreseeable future - You are the guardian of a minor or medically incapacitated consumer who won't need to apply for credit in the foreseeable future **Notes:** - Place a Security Freeze with each of the 3 CRCs[1] individually - With credit frozen, you will need to take special steps when you want to apply for credit	**Duration:** Until you choose to lift it permanently or temporarily Until the minor becomes an adult Until an authorized request is made to permanently remove the freeze

	Requirements	ADD	LIFT	REMOVE
Illinois	Identity Theft Victim	Free**	Free**	Free**
	Age 65 years or older	Free**	$10.00	Free**
	Protected Consumer	$10.00 (Medically incapacitated) Free (Minor under age of 18)	N/A	Free**
	Non-Victim	$10.00	$10.00	Free**

**In order to be eligible for free Security Freeze services, you may be required to provide proof of eligibility by mail.

Credit Card Loss or Fraudulent Charges

Under the FCBA, your liability for unauthorized use of your credit card tops out at $50. However, if you report the loss before your credit card is used, the FCBA says you are not responsible for any charges you didn't authorize. If your credit card number is stolen, but not the card, you are not liable for unauthorized use.

ATM or Debit Card Loss or Fraudulent Transfers.

If you report an ATM or debit card missing before someone uses it, the EFTA says you are not responsible for any unauthorized transactions. If someone uses your ATM or debit card before you report it lost or stolen, your liability depends on how quickly you report it:

If you report:	**Your maximum loss:**
Before any unauthorized charges are made.	$0
Within 2 business days after you learn about the loss or theft.	$50
More than 2 business days after you learn about the loss or theft, but less than 60 calendar days after your statement is sent to you,	$500
More than 60 calendar days after your statement is sent to you.	All the money taken from your ATM/debit card acount, and possibly more; for example, money in accounts linked to your debit account.

If someone makes unauthorized transactions with your debit card number, but your card is not lost, you are not liable for those transactions if you report them within 60 days of your statement being sent to you.

Provided by Transunion

The Fair Credit Reporting Act (FCRA) gives you specific rights when you are, or believe that you are, the victim of identity theft. Here is a brief summary of the rights designed to help you recover from identity theft:

- You have the right to ask the major credit reporting companies to place a Fraud Alert on your credit report. This will let potential creditors and others know that you may be a victim of identity theft. A Fraud Alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You only need to notify one of the three credit reporting companies: as soon as that company processes your Fraud Alert, it will notify the other two, which must then also place Fraud Alerts on your report.

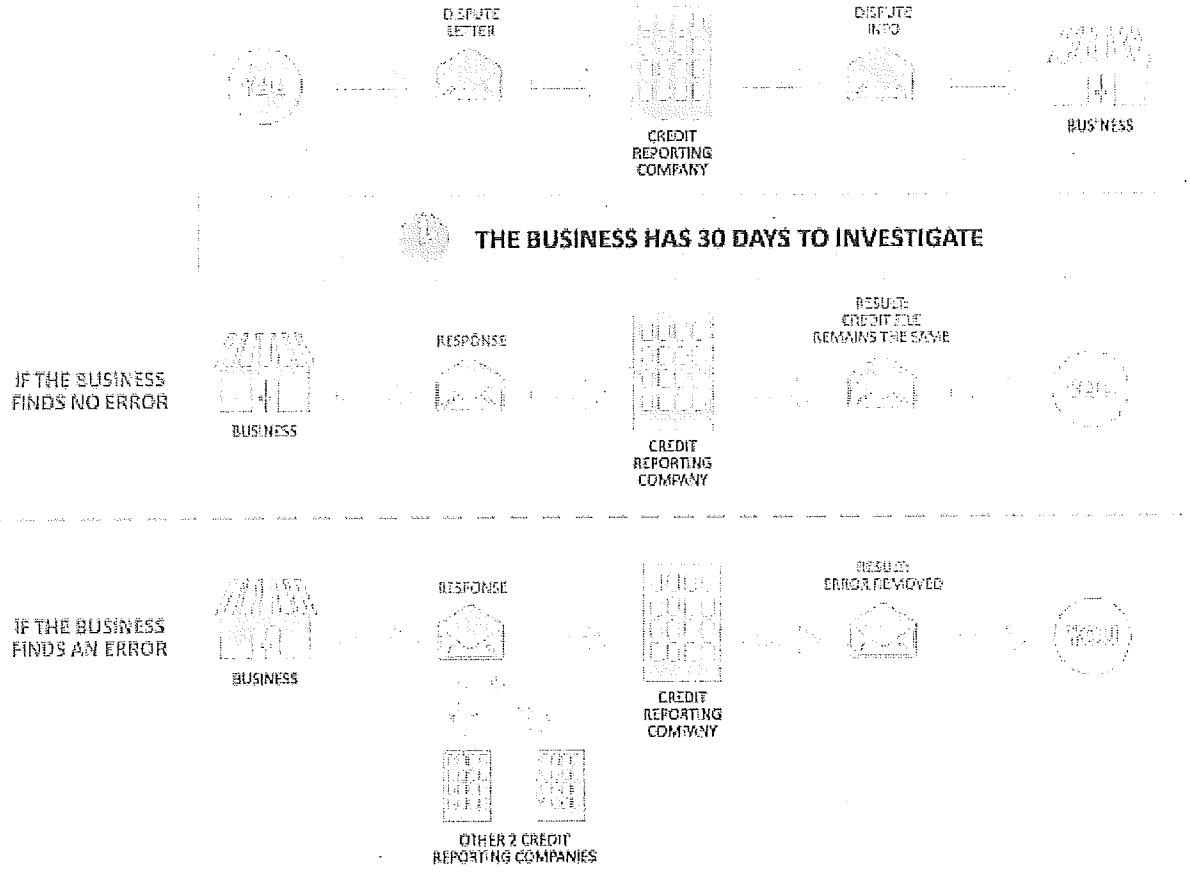
- An Initial Fraud Alert stays on your credit report for at least 90 days. An Extended Alert stays on your report for seven years. To place either of these alerts, you will need to provide appropriate proof of your identity, which may include your Social Security Number. If you ask for an Extended Alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state or local law enforcement agency, plus any additional information requested.
- You have the right to obtain documents relating to fraudulent transactions made or accounts opened using your personal information. A creditor or other business must give you copies of applications and other business records relating to transactions and accounts that resulted from the theft of your identity, if you ask for them in writing. A business may ask you for proof of your identity, a police report and an affidavit before giving you the documents. It also may specify an address for you to send your request. Under certain circumstances, a business can refuse to provide you with these documents.

- You have the right to obtain information from a debt collector. If you ask, a debt collector must provide you with certain information about the debt you believe was incurred in your name by an identity thief, such as the name of the creditor and the amount of the debt.

- If you believe information in your report results from identity theft, you have the right to ask a credit reporting company to block that information from your credit report. An identity thief may run up bills in your name and not pay them. Information about the unpaid bills may appear on your credit report. Should you decide to ask a credit reporting company to block the reporting of this

information, you must identify the information to block, and provide the company with proof of your identity and a copy of your identity theft report. The credit reporting company can refuse or cancel your request for a block if, for example, you don't provide the necessary documentation, or if the block results from an error or a material misrepresentation of fact made by you. If the company declines or rescinds the block, it must notify you. Once a debt resulting from identity theft has been blocked, a person or business with notice of the block may not sell, transfer, or place the debt for collection.

- You also may prevent businesses from reporting information about you to credit reporting companies if you believe the information is a result of identity theft. To do so, you must send your request to the address specified by the business that reports the information to the credit reporting companies. The business will expect you to identify what information you do not want reported and to provide an identity theft report.



VOICE

Victims of Internet Crimes Empowered

GET HELP GET EDUCATED PREVENTION FAQS ABOUT US

GUIDE ME

If you have been a victim of cybercrime, you have a voice.

EVERY DAY MORE THAN ONE MILLION PEOPLE FALL VICTIM TO CYBERCRIME

Prevent your valuable information from being compromised. Research companies before doing business, be aware of prevalent scams, and only use your credit card on secured sites.

LEARN MORE

File a Complaint

TAKE CONTROL

File a complaint directly with the Internet Crime Complaint Center – a partnership between the National White Collar Crime Center (NW3C) and the FBI.

Cybercrime Resources

BE READY

Explore the many cybercrime resources to find the best solution to your cybercrime needs.

Let Us Guide You

WE CAN HELP

Let us take you through a few questions to help narrow down the resources you will need in order to report/resolve your cybercrime.

You have a VOICE let it be heard.

Who We Are

The National White Collar Crime Center (NW3C) is a non-profit organization dedicated to supporting law enforcement in the prevention, investigation, and prosecution of economic and

What We Can Do

Through a combination of training and critical support services, NW3C provides state, local, federal, international and tribal law enforcement agencies with skills and resources needed to

high-tech crimes. While NW3C has no investigative authority itself, the mission of NW3C is to provide training, investigative support and research to agencies and entities involved in the prevention, investigation, and prosecution of economic and high-tech crime.

NW3C currently works with over 5,000 member agencies across the globe, including state, local, federal, international and tribal law enforcement.

NW3C membership consists of law enforcement agencies from the 50 states, U.S. territories and 16 countries.

Made possible by a generous donation from Symantec™, the VOICE (Victims of Internet Crimes Empowered) website serves as a comprehensive, trustworthy source of information for victims of Internet-related crime and the public at large. Through this site, NW3C aims to not only improve outcomes for victims but also to prevent other Internet users from falling victim to cybercrime.

tackle emerging issues regarding economic and cybercrime.

For the general public, NW3C provides information and research so they can protect themselves against economic and cybercrime.

Victims of internet crimes can register complaints through the Internet Crime Complaint Center's website at www.ic3.gov. This process notifies the appropriate authorities at local, state, and federal levels promptly, accurately, and securely, and provides analysts and law enforcement experts a foundation from which to launch an official investigation.

Site Map

Get Help
Get Educated
Prevention
FAQS
About Us
Privacy Statement
Terms of Use

Helpful Links

nw3c.org
ic3.gov
Norton.com

Proud Sponsors